



DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number: 220210-0045]

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; Request for Information.

SUMMARY: The National Institute of Standards and Technology (NIST) is seeking information to assist in evaluating and improving its cybersecurity resources, including the “Framework for Improving Critical Infrastructure Cybersecurity” (the “NIST Cybersecurity Framework,” “CSF” or “Framework”) and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains. NIST is considering updating the NIST Cybersecurity Framework to account for the changing landscape of cybersecurity risks, technologies, and resources. In addition, NIST recently announced it would launch the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains. This wide-ranging public-private partnership will focus on identifying tools and guidance for technology developers and providers, as well as performance-oriented guidance for those acquiring such technology. To inform the direction of the NIICS, including how it might be aligned and integrated with the Cybersecurity Framework, NIST is requesting information that will support the identification and prioritization of supply chain-related cybersecurity needs across sectors. Responses to this RFI will inform a possible revision of the Cybersecurity Framework as well as the NIICS initiative.

DATES: Comments in response to this notice must be received by [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

Submissions received after that date may not be considered.

Comments may be submitted by any of the following methods:

Electronic submission: Submit electronic public comments via the Federal e-Rulemaking Portal.

1. Go to www.regulations.gov and enter NIST-2022-0001 in the search field,
2. Click the “Comment Now!” icon, complete the required fields, and
3. Enter or attach your comments.

Electronic submissions may also be sent as an attachment to CSF-SCRM-RFI@nist.gov and may be in any of the following unlocked formats: HTML; ASCII; Word; RTF; or PDF. Please submit comments only and include your name, organization's name (if any), and cite “NIST Cybersecurity RFI” in all correspondence. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Please do not submit additional materials.

Comments received by the deadline may be posted at www.regulations.gov and <https://www.nist.gov/cyberframework>. All submissions, including attachments and other supporting materials, may become part of the public record and may be subject to public disclosure. NIST reserves the right to publish relevant comments publicly, unedited and in their entirety. Personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Do not submit confidential business information, or otherwise sensitive or protected information.

Comments that contain profanity, vulgarity, threats, or other inappropriate language or

content will not be considered.

FOR FURTHER INFORMATION CONTACT: For questions about this RFI contact: CSF-SCRM-RFI@nist.gov or Katherine MacFarland, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899; (301) 975-3359. Direct media inquiries to NIST's Office of Public Affairs at (301) 975-2762. Users of telecommunication devices for the deaf, or a text telephone, may call the Federal Relay Service, toll free at 1-800-877-8339.

Accessible Format: NIST will make the RFI available in alternate formats, such as Braille or large print, upon request by persons with disabilities.

SUPPLEMENTARY INFORMATION: The NIST Cybersecurity Framework consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to reduce cybersecurity risks. It is used widely by private and public sector organizations in and outside of the United States and has been translated into multiple languages, speaking to its success as a common resource.

The Cybersecurity Framework was last updated in April 2018. Much has changed in the cybersecurity landscape in terms of threats, capabilities, technologies, education and workforce, and the availability of resources to help organizations to better manage cybersecurity risk. That includes an increased awareness of and emphasis on cybersecurity risks in supply chains, including a decision to launch NIICS. With those changes in mind, NIST seeks to build on its efforts to cultivate trust by advancing cybersecurity and privacy standards and guidelines, technology, measurements, and practices by requesting information about the use, adequacy, and timeliness of the Cybersecurity Framework and the degree to which other NIST resources are used in

conjunction with or instead of the Framework. Further, to inform the direction of the NIICS, including how it might be aligned and integrated with the Cybersecurity Framework, NIST is requesting information that will support the identification and prioritization of supply chain-related cybersecurity needs across sectors.

Following is a non-exhaustive list of possible topics that may be addressed in any comments. Comments may address topics in the following list, or any other topic believed to have implications for the improvement of the NIST Cybersecurity Framework or NIST's cybersecurity guidance regarding supply chains. NIST will consider all relevant comments in the development of the revised Framework and guidance regarding supply chains.

Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.
2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?
3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).
4. Any features of the NIST Cybersecurity Framework that should be changed,

added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.
6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.

Relationship of the NIST Cybersecurity Framework to other Risk Management Resources

7. Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:

- Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).
- Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.
- Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST

framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

9. There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline. Cybersecurity Supply Chain Risk Management

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from EO 14028, to increase trust and assurance in technology products, devices, and services?

12. Approaches, tools, standards, guidelines, or other resources necessary for

managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework – or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2022-03642 Filed: 2/18/2022 8:45 am; Publication Date: 2/22/2022]